

- 10 -

REMARKS

The Examiner has rejected Claims 1-3, 5, 7, 9-11, 13, 15, 17-19, 21, and 23 under 35 U.S.C. 102(e) as being anticipated by Marsh (U.S. Patent No. 6,763,462). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims.

With respect to the independent claims, the Examiner has relied on the following excerpt from the Marsh reference to make a prior art showing of applicant's claimed technique where "said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book" and "said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages" (see this or similar, but not necessarily identical language in the independent claims).

"Referring to FIG. 2, the random numbers may be generated when the email application 102 is launched, as shown in block 200. Each time an electronic message is transmitted, the virus detection utility 104 inspects the outgoing message to identify the message's intended recipients. The virus detection utility 104 may examine e-mail distribution patterns by comparing selected e-mail addresses corresponding to the random numbers with potential recipients of the outgoing e-mail message at block 204. If all of the selected e-mail addresses are listed as recipients of a pending electronic message at diamond 206, possible virus activity may be occurring and a user may be notified as shown in block 208. Otherwise, an outgoing electronic message may be delivered according to normal operations of the e-mail application 102 at block 210. In accordance with another embodiment, potential virus activity may be detected by finding a specified number of the e-mail addresses corresponding to the generated random numbers in the recipient list of an outgoing message. For example, a user may be alerted if three (3) of the five (5) e-mail addresses associated with the random numbers are listed as recipients. In this manner, viruses that attempt to spread to other computers rapidly by sending e-mail may be identified by monitoring patterns of e-mail distribution in a user's e-mail account.

A user may be notified of possible virus activity (block 208) through any conventional messaging technique such as a pop-up

- 11 -

warning dialog. A virus warning may include information regarding recent e-mail activity such as recipients and message content. The virus warning may also give a user options to respond to possible virus activity including deleting an outgoing message without sending, saving an outgoing message for later examination, or disregarding the warning and sending an outgoing message.

In yet another embodiment, the virus detection utility 104 may examine e-mail distribution patterns to determine if a computer virus is replicating itself by sending e-mail messages to individual e-mail addresses (i.e., one at a time). Some viruses may attempt to send a series of e-mail messages, each to a different e-mail address, in an effort to disguise a mass distribution of virus code segments. The random numbers generated may again represent positions of an e-mail addresses in a distribution list or address book. In this embodiment, the virus detection utility 104 may track e-mail messages sent by the e-mail application 102. If electronic messages are sent to each of the e-mail addresses represented by the random numbers in a specified period of time, a virus warning may be issued to a user. The user would again have the options described above regarding the disposition of an outgoing message. For example, if e-mail messages are transmitted to all recipients identified by the random numbers within two minutes, a user may be alerted. Alternatively, potential virus activity may be identified if electronic messages are transmitted to a particular number of the selected e-mail addresses (e.g., 3 out of 5) within the specified period of time, e.g. two minutes. (Marsh, Col. 3, Paragraphs 2-4 - emphasis added)

Applicant respectfully asserts that the excerpts from Marsh relied upon by the Examiner merely teach "examin[ing] e-mail distribution patterns by comparing selected e-mail addresses corresponding to the random numbers with potential recipients of the outgoing e-mail message" (emphasis added). Specifically, the excerpt from Marsh discloses detecting potential virus activity when "all of the selected e-mail addresses are listed as recipients of a pending electronic message" (emphasis added) or when "a specified number of the e-mail addresses corresponding to the generated random numbers in the recipient list of an outgoing message" (emphasis added).

However, there is simply not even a suggestion in the excerpt from Marsh of a technique where "said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book" (emphasis added), as claimed by applicant.

- 12 -

Additionally, the excerpts from Marsh fail to meet a technique where “said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages” (emphasis added), as claimed by applicant. There simply is no disclosure in the excerpt from Marsh for a technique of “message content having at least a threshold level of similarity to non-identical message content,” as claimed by applicant.

In the Office Action mailed 02/15/2006, the Examiner argued “that Marsh has (i) and therefore the examiner does not find the argument persuasive.” Applicant respectfully asserts that this rejection is avoided by virtue of the amendments made to the independent claims. Specifically, applicant notes that the claims now clearly require items (i)-(iii). Note amendment below:

“identifying logic operable to identify whether:

(i) said e-mail message is being sent to more than a threshold number of addressees specified within said address book;

(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book; and

(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;

wherein said identifying logic is further operable to identify said email message as potentially containing malware if at least one of items (i), (ii), and (iii) is identified” (emphasis added - see this or similar, but not necessarily identical language in the independent claims).

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628,

- 13 -

631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Marsh reference, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 25-28 below, which are added for full consideration:

"wherein said e-mail message is identified as potentially containing malware only if said e-mail message includes an executable element, to speed processing" (see Claim 25);

"wherein said e-mail message is identified as potentially containing malware when said e-mail message and said previously generated e-mail messages share a common attachment" (see Claim 26);

"wherein a message is sent to a malware computer program provider to provide a warning of new malware outbreaks when said e-mail message is identified as potentially containing malware" (see Claim 27); and

"said message to said malware computer program provider includes a copy of said e-mail message" (see Claim 28).

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

- 14 -

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAIIP462).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100